DEVICE AND SYSTEM FOR VIDEO INPUT

Publication number: JP9200730
Publication date: 1997-07-31
Inventor: OISHI KAZUOMI
Applicant: CANON KK
Classification:
- international: ***H04N5/91; G09C1/00; H03M7/30; H04L9/00; H04L9/32; H04N1/00; H04N7/167;*** **H04N5/91; G09C1/00; H03M7/30; H04L9/00; H04L9/32; H04N1/00; H04N7/167;** (IPC1-7): H03M7/30; H04N7/167; G09C1/00; H04L9/32; H04N5/91
- European: H04L9/32S
Application number: JP19960003603 19960112
Priority number(s): JP19960003603 19960112

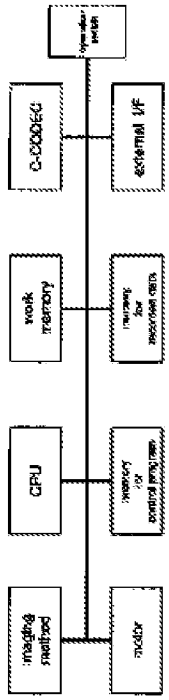
Also published as:

US7000112 (B1)
US2005283612 (A1)

Report a data error here

Abstract of **JP9200730**

PROBLEM TO BE SOLVED: To provide a video input device with which the propriety of formed digital video data can be certified. SOLUTION: This video input device for inputting an image and converting it digital is provided with a digital signature generating part C-CODEC for generating a digital signature for identifying these digital converted video data based on secrecy information (such as a cryptographic key to be used for the digital signature system of a public key encipher system, for example), specific to this video input device and these video data. Then, concerning the formed video data, the digital signature to be generated only by the video input device is found and the video data and the digital signature corresponding to these video data are defined as the output data of the video input device. Thus, any other device excepting for the video input device for forming certain video data can not generate the digital signature corresponding to these video data and when the output data are revised or forged, it can be detected.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－200730

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｎ	7/167			Ｈ０４Ｎ	7/167	
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ
			7259－5Ｊ			６４０Ｄ
Ｈ０４Ｌ	9/32		9382－5Ｋ	Ｈ０３Ｍ	7/30	Ｚ
Ｈ０４Ｎ	5/91			Ｈ０４Ｌ	9/00	６７５Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全 12 頁）　最終頁に続く

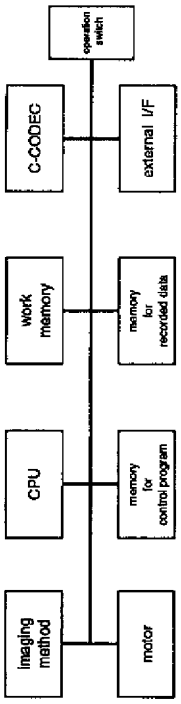
(21)出願番号　特願平8－3603

(22)出願日　平成８年(1996)１月12日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　大石　和臣
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　映像入力装置および映像入力システム

(57)【要約】
【課題】　形成されたディジタル映像データの正当性を認証することを可能にする映像入力装置を提供する。
【解決手段】　映像を入力してディジタル変換する映像入力装置において、上記映像入力装置に固有の秘密情報（例えば、公開鍵暗号系のディジタル署名方式で使用される秘密鍵）と、上記ディジタル変換された映像データとに基づき、上記映像データを識別するディジタル署名を生成するディジタル署名生成部C-CODECを設け、形成した映像データに対して、映像入力装置だけが生成できるディジタル署名を求め、映像データとそれに対応するディジタル署名とを映像入力装置の出力データとすることにより、ある映像データを形成する映像入力装置以外のものがそれに対応するディジタル署名を生成できないようにするとともに、出力データに対して改ざんや偽造がなされたときは、それを検出できるようにする。



【特許請求の範囲】
【請求項１】　映像を入力してディジタル・データに変換する映像入力装置において、
上記映像入力装置に固有の秘密情報および上記映像入力装置に接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたディジタル・データとに基づき、所定の演算を実行し、上記ディジタル・データを識別する情報を生成する手段を有することを特徴とする映像入力装置。
【請求項２】　上記所定の演算として、公開鍵暗号系を用いるディジタル署名方式の演算を実行することを特徴とする請求項１に記載の映像入力装置。
【請求項３】　上記所定の演算を、上記映像入力装置の内部および上記映像入力装置に接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項１または２に記載の映像入力装置。
【請求項４】　上記映像入力装置に入力され変換されたディジタル・データに対して圧縮変換を行なう手段と、上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項１～３の何れか１項に記載の映像入力装置。
【請求項５】　映像を入力してディジタル・データに変換する映像入力システムにおいて、
上記映像入力システムに固有の秘密情報および上記映像入力システムに接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたディジタル・データとに基づき、所定の演算を実行し、上記ディジタル・データを識別する情報を生成する手段と、
上記ディジタル・データを識別する情報を用いて、上記生成されたディジタル・データが確かに上記映像入力システムで生成されたものかどうかを検証する手段とを有することを特徴とする映像入力システム。
【請求項６】　上記所定の演算として、公開鍵暗号系を用いるディジタル署名方式の演算を実行することを特徴とする請求項５に記載の映像入力システム。
【請求項７】　上記所定の演算を、上記映像入力システムの内部および上記映像入力システムに接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項５または６に記載の映像入力システム。
【請求項８】　上記映像入力システムに入力され変換されたディジタル・データに対して圧縮変換を行なう手段と、
上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項５～７の何れか１項に記載の映像入力システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、映像入力装置および映像入力システムに関する。
【０００２】
【従来の技術】映像を入力してディジタルの映像データを形成する映像入力装置や映像入力システムは、映像データの高精細化および高画質化と、装置あるいはシステムの低コスト化とが追求されることが一般的である。そのために、高解像度の入力デバイスや効率の良い符号化、および小型化のための技術等が広範に研究開発されている。
【０００３】これに対し、形成されたディジタルの映像データが確かにその映像入力装置あるいは映像入力システムで形成されたことを保証する技術を機能として組み込むことは、従来あまり考えられていなかった。
【０００４】
【発明が解決しようとする課題】アナログの映像入力装置では、形成される映像はアナログ・データであるため、その映像データの改ざんあるいは偽造を行うためには特殊な知識、能力等が必要であり、結果的に改ざんや偽造が成功することは少なかった。これに対して、ディジタルの映像データの場合は、比較的容易に改ざんや偽造が行なわれ得るため、映像データの信憑性が低いという問題があった。
【０００５】例えば、銀塩写真のネガ・フィルムに記憶されている映像は、銀塩分子により構成されているため、これを見破って改ざんや偽造を行うことは困難である。これに対して、ディジタル・データで表現されている映像は、０と１のビット列から構成されているため、コンピュータを用いて改ざんや偽造が行なわれやすい。したがって、ディジタルの映像データは、事実の証拠としての証明能力が小さい、すなわち信憑性が低いと言え、用途が限定される恐れがある。
【０００６】本発明はこのような問題を解決するために成されたものであり、形成されたディジタル映像データの正当性を認証することができるようにした映像入力装置および映像入力システムを提供することを目的とする。
【０００７】
【課題を解決するための手段】本発明の映像入力装置およびシステムは、ディジタル・データの正当性を保証するための技術であるディジタル署名を応用する。ディジタル署名とは、岡本栄司著の暗号理論入門（共立出版株式会社）によれば、「メッセージや情報の作成者が確かにそれらを作成したことを示す」ものである。つまり、ユーザや、計算機等の通信または計算処理を行なう主体（エンティティと呼ぶ）があるディジタル・データを認めたときに、その事実を示す証拠として用いられるディジタル・データである。
【０００８】本発明の映像入力装置は、形成したディジタルの映像データに対して、映像入力装置だけが生成できるディジタル署名を求め、映像データ自体とそれに対応するディジタル署名とを映像入力装置の出力データと

する。そして、本発明の映像入力システムにおいて、上記出力データを受け取ったエンティティは、映像データとディジタル署名との対応関係が正しく成り立つかどうかを確認し、正しい対応関係が認められないデータは正当ではないとする。

【０００９】上述の手段により、あるディジタル映像データを形成する映像入力装置以外のものは、その映像データに対応するディジタル署名を生成することはできず、かつ、出力データに対して改ざんや偽造がなされたときは、それを検出することが可能になる。したがって、その映像データが確かにその映像入力装置で生成されたものだということを保証することが可能になり、ディジタル映像データに事実の証拠としての証明能力を与えることができる。

【００１０】

【発明の実施の形態】

〔第１の実施形態〕本実施形態では、ディジタル署名のアルゴリズムとして公開鍵暗号を用い、映像入力装置の内部に固有の秘密情報として公開鍵暗号を有する場合について説明する。ただし、これは１つの例であり、公開鍵暗号を用いるディジタル署名アルゴリズムの代わりに、元情報と秘密情報とに基づいて元情報を識別する情報を生成する手段を有するものは本実施形態に全て含まれる。

【００１１】以下では、最初に公開鍵暗号について説明する。次に、映像入力装置の構成について説明し、公開鍵暗号を用いたディジタル署名を適用した本実施形態の映像入力装置がディジタル署名を生成するときの具体的な手続きを述べる。最後に、映像入力システムの機能の一部として、そのディジタル署名を検証するときの具体的な手続きについて説明する。

【００１２】公開鍵暗号

公開鍵暗号とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開するとともに復号鍵を秘密に保持する暗号方式である。公開鍵暗号は、送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現でき、ディジタル署名を実現する有力な技術だと考えられている。

【００１３】例えば、通信文Ｍに対して、公開の暗号鍵k_pを用いて行う暗号化操作を$E(k_p, M)$とし、秘密の復号鍵k_Sを用いて行う復号操作を$D(k_S, M)$とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

（１）暗号鍵k_pが与えられたとき、暗号化操作$E(k_p, M)$の計算は容易である。また、復号鍵k_Sが与えられたとき、復号操作$D(k_S, M)$の計算は容易である。

（２）もしユーザが復号鍵k_Sを知らないなら、暗号鍵k_pと暗号化操作$E(k_p, M)$の計算手順とＣ＝$E(k_p, M)$とを知っていても、通信文Ｍを決定することは計算量の点で困難である。

【００１４】次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより秘密通信機能が実現できる。

（３）全ての通信文（平文）Ｍに対し暗号化操作$E(k_p, M)$が定義でき、

$D(k_S, E(k_p, M)) = M$

が成立する。つまり、暗号鍵k_pは公開されているため誰もが暗号化操作$E(k_p, M)$の計算を行うことができるが、$D(k_S, E(k_p, M))$の計算をして通信文Ｍを得ることができるのは復号鍵k_Sを持っている本人だけである。

【００１５】一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証機能が実現できる。

（４）全ての通信文（平文）Ｍに対し復号操作Ｄ(k_S, M)が定義でき、

$E(k_p, D(k_S, M)) = M$

が成立する。

【００１６】つまり、復号操作$D(k_S, M)$の計算ができるのは復号鍵k_Sを持っている本人のみであり、他の人が偽の秘密鍵k_S'を用いて$D(k_S', M)$の計算を行い、復号鍵k_Sを持っている本人になりすましたとしても、

$E(k_p, D(k_S', M)) \neq M$

なので、受信者は受けとった情報が不正なものであることを認識できる。また、$D(k_S, M)$の値が改ざんされても$E(k_p, D(k_S, M)') \neq M$となり、受信者は受けとった情報が不正なものであることを確認できる。この復号操作$D(k_S, M)$を通信文Ｍに対するディジタル署名と呼ぶ。

【００１７】以下に、代表的な公開鍵暗号方式を挙げる。上述の秘密通信と認証通信とを行うことがができる方式として、ＲＳＡ暗号（R.L.Rivest,A.Shamir and L.Adleman:“A method of obtaining digital sinnatures and public key cryptosystems ”,Comm. of ACM 1987）、Ｒ暗号（M.Rabin:“Digitalized signatures and public-key cryptosystems ”,MIT/LCS/TR-212,Technical Report MIT.1979 ）、Ｗ暗号（H.C.Williams: “A modification of the RSA public-key encryption procedure ”,IEEE Trans. Inf. Theory,IT-26,6,1980 ）、ＭＩ暗号（松本，今井：“公開鍵暗号系の新しいアルゴリズム”，信学技報，IT82-84,1982;T.Matsumoto and H.Imai:“A class of asymmetriccryptosystems based on polynomials over finite rings”,IEEE International Symp. on Infomation Theory,1983 ）などがある。

【００１８】また、秘密通信のみができる方式として、ＭＨ暗号（R.C.Merkle and M.E.Hellman: “Hidding infomation and signatures in trapdoor knapsacks ”,IEEETrans. Inf. Theory,IT-24,5,1987 ）、ＧＳ信号

（A.Shamir and R.E.Zippel:“On the security of the Merkle-Hellman cryptographic schme ”,IEEE Trans. Inf. Theory,IT-26,3,1980 ）、ＣＲ暗号（B.Chor and R.L.Rivest:“A knapsack type public key cryptosystems based on arithmetric in finit field”,Proc. Crypto84 ）、M暗号（R.J.McEliece: “A public-key cryptosystem based on algebraic cording theory ”DSN Progress Rwp.,Jet Propulsion Lab.,1978）、Ｅ暗号（T.E.ElGamal:“A Public key cryptosystem and a signature scheme based on discretre logarithm ”,Proc. Crypto 84,1984 ）、Ｔ暗号（辻井重男、“行列分解を利用した公開鍵暗号の一方式”，信学技報，IT85-12,1985）などがある。

【００１９】さらに、認証通信のみができる方式として、Ｓ暗号（A.Shamir: “A fast signature scheme ”,Report MIT/LCS/TM-107,MIT laboratory for computer science,Cambridge,Mass.,1978 ）、Ｌ暗号（K.Lieberherr：“Uniform complexity and digital signature”,Lecture Notes in Computer Science 115 Automata,Language and programming,Eighth Colloquium Acre,Israel,1981 ）、ＧＭＹ暗号（S.Goldwasser,S.Micali and A.Yao:“Strong signature schemes”,ACM Symp.on Theory of Computing,1983）、ＧＭＲ暗号（S.Goldwasser,S.Micali and R.L.Rivest: “A “paradoxical ”solution to the signature problem ”,ACM Symp. on Foundation of Computer Science,1984 ）、ＯＳＳ暗号（H.Ong,C.P.Schnorr and A.Shamir.:“An efficient signature scheme based on quadratic equation ”,ACM Symo. on Theory of Computing 1984）、ＯＳ暗号（岡本、白井、：“多項式演算によるディジタル署名方式、信学論（Ｄ）、J68-D,5,1985;T.Okamoto and A.Shiraisi:“A fast signature scheme based on quadratic inequaliteis ”,IEEE Symp. on Theory of Computing,1984 ）などがある。

【００２０】映像入力装置の構成

次に、上記のような公開鍵暗号を用いたディジタル署名を適用した本実施形態の映像入力装置について、図１を用いて説明する。図１に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。imaging methodは撮像部であり、対象となる被写体を撮影して電気信号に変換し、適当な信号処理、Ａ／Ｄ変換処理、画像処理、情報源符号化処理等を行ない、ディジタル・データを出力する。

【００２１】ＣＰＵは中央演算装置であり、memory for control programに記憶されている制御ソフトウェアに従い、所定の計算および制御を行なう。上記memory for control programはメモリ部であり、上記制御ソフトフェアを記憶する。work memory はメモリ部であり、ＣＰＵが計算を行なうための作業用に使われる。operation switchは操作部であり、装置を使用するユーザが種々の指示を入力するためのものである。

【００２２】motor は機構動作部であり、ＣＰＵの制御に応じて図示しない機械的な動作機構を制御する。memory for recorded dataはメモリ部であり、本装置が出力する映像データあるいはその一部を記録する。external I/Fは、コンピュータあるいは着脱可能なメモリ等の外部装置とのインターフェイス部であり、映像データや制御ソフトウェア等を上記外部装置との間で通信する。C-CODEC はディジタル署名生成部であり、入力されたディジタル・データに対するディジタル署名を生成する。

【００２３】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、操作者は、操作部operation switchからその指示を入力する。ＣＰＵは、その撮影指示と、メモリ部memory for control programに記憶されている制御ソフトウェアとに従って、撮像部imaging methodや機構動作部motor を制御して対象を撮影し、その撮影により形成された映像のディジタル・データをディジタル署名生成部C-CODEC に入力する。ディジタル署名生成部C-CODEC は、入力されたディジタル・データに対応するディジタル署名を生成する。

【００２４】そして、このようにして形成された映像データとそれに対応するディジタル署名は、操作者からの指示に応じて、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたディジタル・データが一度メモリ部memory for recorded dataに記録された後にディジタル署名生成部C-CODEC に入力されることもあり得る。

【００２５】次に、以上のような映像入力装置に対して公開鍵暗号を用いるディジタル署名を適用して、装置内に固有の秘密情報として秘密鍵を有する場合について説明する。

【００２６】本実施形態による映像入力装置の秘密鍵（復号鍵）をsk_{cam}、ディジタル署名生成アルゴリズムをD_{cam}、公開鍵（暗号鍵）をpk_{cam}、ディジタル署名検証アルゴリズムをE_{cam}とする。秘密鍵sk_{cam}とディジタル署名生成アルゴリズムD_{cam}は、ディジタル署名生成部C-CODEC の内部に記憶されている。また、公開鍵pk_{cam}とディジタル署名検証アルゴリズムE_{cam}は、少なくともデータの正当性を確認するエンティティ（検証者と呼ぶ）には知られている。

【００２７】上記のような映像入力装置において、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【００２８】ディジタル署名生成

本実施形態の映像入力装置で形成されたディジタル映像データＩは、ディジタル署名生成部C-CODEC に入力される。ディジタル署名生成部C-CODEC は、その内部に記憶

されている秘密鍵sk_{cam}とディジタル署名生成アルゴリズムD_{cam}とを用いてD_{cam}（sk_{cam}，Ｉ）を計算し、ディジタル署名として出力する。そして、このようにして得られる映像データＩとディジタル署名D_{cam}（sk_{cam}，Ｉ）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００２９】また、映像データとそれに対応するディジタル署名とが確かに上記の映像入力装置によって入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。なお、映像入力装置に加えて以下に述べる検証の手続きも含めたシステム全体を、映像入力システムという。

【００３０】ディジタル署名検証

映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，Ｉ）を受け取った検証者は、公開鍵pk_{cam}とディジタル署名検証アルゴリズムE_{cam}とを用いて、

Ｉ′＝E_{cam}（pk_{cam}，D'_{cam}（sk_{cam}，Ｉ））

が成り立つかどうかを確認する。

【００３１】ここで、上式が成立した場合は、受け取った映像データＩ′は上記映像入力装置で撮影された映像データＩである。一方、上式が成立しない場合は、受け取った映像データＩ′が上記映像入力装置で撮影された映像データＩではない映像になっている。すなわち、D'_{cam}（sk_{cam}，Ｉ）の値がD_{cam}（sk_{cam}，Ｉ）の値とは異なる、あるいは映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，Ｉ）との両方が異なる、のいずれかの場合であり、上記装置で撮影、形成された映像データではないと判断することができる。

【００３２】〔第２の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図１を用いて説明する。

【００３３】本実施形態においては、次に述べる外部装置としての携帯装置（図示せず）に収められている秘密鍵をsk_{man}、ディジタル署名生成アルゴリズムをD_{man}とし、対応する公開鍵をpk_{man}、ディジタル署名検証アルゴリズムをE_{man}とする。また、上記携帯装置は、携帯型の情報処理装置であり、撮影の際には、外部装置とのインターフェイスexternal I/Fを介して映像入力装置に接続されるものである。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}とを知っている。

【００３４】映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、上記携帯装置は映像入力装置内の外部装置とのインターフェイスexternal I/Fに接続され、撮影者は、操作部operation　switchから撮影の指示を入力する。ＣＰＵは、その撮影指示と、メモリ部memory for control programに記憶されている制御ソフトウェアに従って、撮像部imaging methodや機構動作部motor を制御して対象を撮影し、それにより得られる映像のディジタル・データをディジタル署名生成部C-CODEC に入力する。

【００３５】ＣＰＵと携帯装置は、外部装置とのインターフェイスexternal I/Fを介して通信する。これにより、ディジタル署名生成部C-CODEC は、携帯装置に記憶されている秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを得て、これらの情報を用いて、上記撮影して形成された映像データに対するディジタル署名を求める。

【００３６】このようにして形成された映像データとそれに対応するディジタル署名は、操作者からの指示に応じて、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたディジタル・データが一度メモリ部memory for recorded dataに記録された後にディジタル署名生成部C-CODEC に入力されることもあり得る。

【００３７】以上のような映像入力装置において、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【００３８】ディジタル署名生成

ＣＰＵは、外部装置とのインターフェイスexternal I/Fを介して携帯装置から秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを映像入力装置内のメモリ部work memory とＣＰＵとにダウンロードする。次に、映像入力装置内で形成されたディジタル映像データＩを用いてD_{man}（sk_{man}，Ｉ）を計算し、それをディジタル署名として出力する。そして、このようにして得られる映像データＩとディジタル署名D_{man}（sk_{man}，Ｉ）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００３９】また、映像データとそれに対応するディジタル署名とが確かに上記の携帯装置が接続されたときに入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。

【００４０】ディジタル署名検証

記録データ（映像データＩ′とディジタル署名D'_{man}（sk_{man}，Ｉ）とする）を受け取った検証者は、ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}とを用いて、

Ｉ′＝E_{man}（pk_{man}，D'_{man}（sk_{man}，Ｉ））

が成り立つかどうかを確認する。

【００４１】ここで、上式が成立した場合は、記録デー

タの映像Ｉ′は上記携帯装置が接続されたときに撮影された映像Ｉである。一方、上式が成立しない場合は、記録データの映像Ｉ′が上記携帯装置が接続されたときに撮影された映像Ｉではない映像になっている。すなわち、D'_{man}（sk_{man}，Ｉ）の値がD_{man}（sk_{man}，Ｉ）の値とは異なる、あるいは映像データＩ′とディジタル署名D'_{man}（sk_{man}，Ｉ）との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに撮影された映像データではないと判断することができる。

【００４２】したがって、このような映像入力システムにおいて、携帯装置が撮影者と正確に一対一に対応していれば、撮影者が撮影した映像であることを保証するシステムが実現できる。

【００４３】〔第３の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有するとともに、その携帯装置が演算能力を持ち、ディジタル署名生成の手続きを以下のように行う場合について、図１を用いて説明する。

【００４４】ディジタル署名生成

ＣＰＵは、映像入力装置内で形成されたディジタル映像データＩを、外部装置とのインターフェイスexternal Ｉ/Fを介して携帯装置に送る。携帯装置は、その内部に記憶されている秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを用いて、送られて来た映像データＩからディジタル署名D_{man}（sk_{man}，Ｉ）を計算し、それを外部装置とのインターフェイスexternal I/Fを介して映像入力装置に送る。

【００４５】そして、このようにして得られた映像データＩとディジタル署名D_{man}（sk_{man}，Ｉ）は、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００４６】ディジタル署名検証

第２の実施形態と同じであるので、説明を省略する。

【００４７】〔第４の実施形態〕本実施形態では、ディジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置とその外部装置である携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図１を用いて説明する。なお、本実施形態の処理は、以下のディジタル署名生成と検証の処理を除いて、第１の実施形態および第２の実施形態と同じである。

【００４８】ディジタル署名生成

ＣＰＵは、外部装置とのインターフェイスexternal I/Fを介して携帯装置から秘密鍵sk_{man}とディジタル署名生成アルゴリズムD_{man}とを映像入力装置内のメモリ部work memory とＣＰＵとにダウンロードする。次に、上記映像入力装置内で形成されたディジタル映像データＩからD_{man}（sk_{man}，Ｉ）を計算し、その計算結果をディジタル署名生成部C-CODEC に入力する。

【００４９】ディジタル署名生成部C-CODEC は、入力されたデータD_{man}（sk_{man}，Ｉ）に対し、D_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））の計算を実行し、その計算結果をディジタル署名として出力する。このようにして形成された映像データＩとディジタル署名D_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））とは、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００５０】また、映像データとそれに対応するディジタル署名とが確かに上記携帯装置が接続されたときに上記映像入力装置で入力された映像であるか否かを検証する具体的な手続きは、以下のようになる。

【００５１】ディジタル署名検証

記録データ（映像データＩ′とディジタル署名D'_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））とする）を受け取った検証者は、映像入力装置に固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を用いて、

Ｉ′＝E_{man}（pk_{man}，E_{cam}（pk_{cam}，D'_{cam}（sk_{cam}，D_{man}（sk_{man}，Ｉ））））

が成り立つかどうかを確認する。

【００５２】ここで、上式が成立した場合は、記録データの映像Ｉ′は上記映像入力装置で上記携帯装置が接続されたときに撮影された映像であるが、上式が成立しない場合はそれとは異なる映像であると判断することができる。

【００５３】なお、上記の実施形態では、ディジタル署名生成の順序は、最初に携帯装置で次に映像入力装置の順であったが、逆にすることも可能であり、その場合は検証の順序も逆になる。また、映像入力装置と携帯装置との両方が署名したデータをその順序にかかわりなく生成、検証することも可能である。さらに、携帯装置のディジタル署名生成アルゴリズムD_{man}を映像入力装置の内部に記憶しておき、秘密鍵sk_{man}のみを携帯装置に記憶しておくこともできる。

【００５４】〔第５の実施形態〕次に、圧縮技術を用いて、記録する映像データの代わりにそれを圧縮したデータに対してディジタル署名を生成する場合について説明する。ここでは、圧縮変換をｃで表すこととする。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、この圧縮変換ｃを知っている。その他は、上記第１～第４の実施形態と同様である。

【００５５】ディジタル署名生成

ＣＰＵは、映像入力装置内の撮像部imaging methodで形成されたディジタル映像データＩに対しｃ（Ｉ）の計算を実行し、それにより得られる圧縮データｃ（Ｉ）を映

像データＩの代わりに用いる。他の処理は、上記第１～第４の実施形態と同様である。例えば、第１の実施形態の場合に即して説明すると、映像データＩとディジタル署名D_{cam}（sk_{cam}，ｃ（Ｉ））とがメモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００５６】ディジタル署名検証

記録データ（映像データＩ´とディジタル署名D'_{cam}（sk_{cam}，ｃ（Ｉ）とする）を受け取った検証者は、ディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}とを用いて、

$c(I') = E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, c(I)))$

が成り立つかどうかを確認する。なお、検証者が圧縮変換の逆変換c^{-1}を知っているならば、

$I' = c^{-1}(E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, c(I))))$

が成り立つかどうかをを確認してもよい。

【００５７】ここで、上式が成立した場合は、記録データの映像Ｉ´は上記映像入力装置で撮影された映像である。一方、上式が成立しない場合は、記録データの映像Ｉ´が上記映像入力装置で撮影された映像Ｉではない映像になっている。すなわち、D'_{cam}（sk_{cam}，ｃ（Ｉ））の値がD_{cam}（sk_{cam}，ｃ（Ｉ）の値とは異なる、あるいは映像データＩ´とディジタル署名D'_{cam}（sk_{cam}，ｃ（Ｉ））との両方が異なる、のいずれかの場合であり、上記映像入力装置で撮影、形成された映像データではないと判断することができる。

【００５８】〔第６の実施形態〕本実施形態では、映像入力装置の一例としてディジタル・カメラを取り上げ、ディジタル署名アルゴリズムとして公開鍵暗号を用い、ディジタル・カメラと携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図２を用いて説明する。

【００５９】ディジタル・カメラの構成

図２に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。ＩＭＧは撮像部であり、対象となる被写体を撮影して電気信号に変換する。ＰＲＣは画像処理部であり、上記撮像部ＩＭＧで形成された電気映像信号に対して適当な信号処理、Ａ／Ｄ変換処理、画像処理、情報源符号化処理等を行ない、ディジタル・カメラからの出力となるディジタル・データを形成する。

【００６０】ＣＰＵは中央演算装置であり、ＲＯＭに記憶されている制御ソフトウェアに従い、ＤＲＡＭを計算用の領域として利用しながら所定の計算を行ない、バスを介してカメラ全体の制御を行なう。上記ＲＯＭは読みだし専用のメモリ部であり、制御プログラムや圧縮変換、表示データなどの、カメラの制御に必要な制御ソフトウェアを記憶する。上記ＤＲＡＭは読み書き可能なメモリ部であり、ＣＰＵが計算を行なうための作業用に使われる。

【００６１】ＳＴＲＧはメモリ部であり、撮影した映像データや音声データあるいはその一部を記録する。ＣＯＤＥＣはディジタル署名生成部であり、秘密鍵と署名生成アルゴリズムとを記憶しており、これらを用いて、入力されたディジタル・映像データに対するディジタル署名を生成する。

【００６２】Ｉ／Ｆは外部装置とのインターフェイス、ＰＣＭＣＩＡは外部装置とのＰＣＭＣＩＡ規格に基づくインターフェイスであり、本実施形態の映像入力装置は、これらのインタフェースを介して映像データ、制御ソフトウェア、状況データ等をコンピュータやメモリ等の外部装置と通信する。ＭＩＣは音声入力部であり、音声を収集し電気信号に変換する。ＯＰ－ＳＷは操作部、ＬＣＤはディスプレイ、ＬＥＤはランプであり、これらを用いてユーザは必要な情報の入出力を行い、カメラを操作する。

【００６３】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、携帯装置はカメラ内の外部装置とのインターフェイスＩ／Ｆに接続され、撮影者は、操作部ＯＰ－ＳＷから撮影の指示を入力する。

【００６４】ＣＰＵと携帯装置は、外部装置とのインターフェイスＩ／Ｆを介して通信し、携帯装置に記憶されている秘密鍵とディジタル署名生成アルゴリズム、およびカメラ内に記憶されている秘密鍵とディジタル署名生成アルゴリズムを用いて、撮影して形成された映像、音声のディジタル・データを圧縮したデータに対するディジタル署名を求める。

【００６５】上記撮影した映像データと録音した音声データとは、操作者からの指示に応じてメモリ部ＳＴＲＧに記録されるか、外部装置とのインターフェイスを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影、録音して形成されたディジタル・データが一度メモリ部ＳＴＲＧに記録された後にディジタル署名が生成されることもあり得る。

【００６６】ここで、本実施形態のディジタル・カメラにおけるディジタル署名生成アルゴリズムをD_{can}、秘密鍵をsk_{cam}、ディジタル署名検証アルゴリズムをE_{cam}、公開鍵をpk_{cam}とする。上記ディジタル署名生成アルゴリズムD_{cam}と秘密鍵sk_{cam}は、ディジタル署名生成部ＣＯＤＥＣの内部に記憶されている。また、圧縮変換アルゴリズムｈはＲＯＭに記憶されている。

【００６７】また、携帯装置に収められている秘密鍵をsk_{man}、ディジタル署名生成アルゴリズムをD_{man}とし、対応する公開鍵をpk_{man}、ディジタル署名検証アルゴリズムをE_{man}とする。上記ディジタル・カメラに固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵

pk_{cam} 、上記携帯装置に固有のディジタル署名検証のアルゴリズムE_{man}と公開鍵pk_{man} 、および圧縮変換アルゴリズムｈは、少なくともデータの正当性を確認するエンティティ（検証者と呼ぶ）には知られている。

【００６８】上記のようなディジタル・カメラにおいて、ディジタル署名が生成されるときの具体的な手続きは次のようになる。

【００６９】ディジタル署名生成

ＣＰＵは、ディジタル・カメラで形成されたディジタル映像及び音声データＩからデータD_{cam}（sk_{cam}，ｈ（Ｉ））を生成し、それを外部装置とのインターフェイスＩ／Ｆを介して携帯装置に送る。携帯装置は、秘密鍵sk_{man}とディジタル署名生成アルゴリズムとD_{man}を用いて、送られて来たデータD_{cam}（sk_{cam}，ｈ（Ｉ））を用いてD_{man}（sk_{man}，D_{can}（sk_{cam}，ｈ（Ｉ））の計算を実行し、その計算結果を、外部装置とのインターフェイスexternal I/Fを介してカメラに送る。

【００７０】そして、このようにして形成されたディジタル・データＩとディジタル署名D_{man}（sk_{man}，D_{cam}（sk_{cam}，ｈ（Ｉ））は、メモリ部ＳＴＲＧに記録されるか、外部装置とのインターフェイスＰＣＭＣＩＡを介して外部装置に送られるか、あるいはその両方が行なわれる。

【００７１】また、撮影されたデータとそれに対応するディジタル署名とが確かに上記携帯装置が接続されたときに上記カメラで撮影されたデータであるか否かを検証する具体的な手続きは、以下のようになる。

【００７２】ディジタル署名検証

記録データ（ディジタル・データＩ´とディジタル署名D'_{man}（sk_{man}，D_{cam}（sk_{cam}，ｈ（Ｉ））とする）を受け取った検証者は、携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}、カメラに固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および圧縮変換アルゴリズムｈを用いて、

ｈ（Ｉ´）＝E_{cam}（pk_{cam}，E_{man}（pk_{man}，D'_{man}（sk_{man}，D_{can}（sk_{cam}，ｈ（Ｉ））））））

が成り立つかどうかを確認する。

【００７３】ここで、上式が成立した場合は、記録データＩ´は上記携帯装置が接続されたときに上記カメラで撮影されたデータである。一方、上式が成立しない場合は、記録データＩ´が上記携帯装置が接続されたときに上記カメラで撮影されたデータＩではないデータになっている。すなわち、D'_{man}（sk_{man}，Ｉ）の値がD_{man}（sk_{man}，Ｉ）の値とは異なる、あるいはディジタル・データＩ´とディジタル署名D'_{man}（sk_{man}，Ｉ）との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに上記カメラで撮影されたデータではないと判断することができる。

【００７４】〔その他の実施形態〕以上に説明した第１～第６の実施形態の組合せで得られる全ての映像入力装置および映像入力システムは、本発明の対象に含まれる。映像入力装置に加えて検証の手続きも含めた映像入力システムの概念図を、図３に示す。

【００７５】図３において、image input deviceは第１～第６の実施形態の映像入力装置、portable deviceは携帯装置であり、これらはexternal I/Fを介して接続されている。また、check deviceはディジタル署名検証処理を実行するための装置、portble device2 はportable device と同様の携帯装置であり、Ｉ／Ｆを介して接続される。

【００７６】例えば、検証装置check deviceは、映像入力装置に固有のディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および携帯装置に固有のディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を読み込んだパーソナル・コンピュータ、あるいは、上記ディジタル署名検証アルゴリズムE_{cam}と公開鍵pk_{cam}、および上記ディジタル署名検証アルゴリズムE_{man}と公開鍵pk_{man}を格納した携帯装置portable device2を接続したパーソナル・コンピュータである。

【００７７】Image は撮影の対象であり、映像入力装置が撮影対象Image を撮影して形成したディジタル映像データがＩである。なお、上記携帯装置portable device2と同等の携帯装置portable device をexternal I/Fを介して接続した映像入力装置image input deviceが検証装置check deviceとなることも可能である。

【００７８】映像データＩは（必要ならば圧縮され、それから）ディジタル署名生成部C-CODEC および外部装置とのインタフェースexternal I/Fを介して携帯装置portabledevice の少なくとも一方に入力されるか、ディジタル署名生成部C-CODEC とインタフェースexternal I/Fとの間で入出力されるか、あるいはその両方が行われる。

【００７９】○印で囲んだ＋の記号は、入力を合成する処理を示し、ディジタル署名生成部C-CODEC および携帯装置portable device の少なくとも一方からの最終出力と、映像データＩとを合成して出力する。このときの出力形式の例を、図４に示す。図４は、映像データＩとその映像データＩに対するディジタル署名とが連結されてひとまとまりにされている状態である。

【００８０】なお、以上の実施形態では、映像データＩとその映像データＩに対するディジタル署名とが出力された。これに対し、ＲＳＡ暗号のようにディジタル署名から元の情報を復元できるアルゴリズムを用いる場合は、映像データＩが圧縮されていないならばディジタル署名のみを記録するか、外部装置に送るか、あるいはその両方を行えばよい。この場合の例を、図５に示す。また、このときの出力形式の例を図６に示す。

【００８１】なお、本発明の対象は、第６の実施形態で述べたディジタル・カメラに限られない。例えば、スキャナ、複写機、ファクシミリ、ファイリング・システム、ＯＣＲ装置等の映像入力装置に本発明を適用可能であり、それらに対応する検証手段を含めた映像入力システムは、全て本発明の対象に含まれる。また、対象とするデータも映像に限らず、音声、文字情報等の一般的な情報に適用できることは言うまでもない。

【００８２】

【発明の効果】以上説明したように、本発明によれば、映像入力装置あるいはそれに接続される外部装置を保持している操作者でないものは映像データに対応するディジタル署名を生成することができず、かつ、出力データに対して改ざんや偽造がなされたときは、上記装置あるいは上記撮影者の公開鍵を用いてそれらを検出するようにシステム全体を構成、運用することが可能になる。

【００８３】したがって、その映像データが確かにその映像入力装置で生成された、あるいはその外部装置を保持している操作者によって撮影されたデータだということを保証することが可能になり、ディジタル映像データに事実の証拠としての証明能力を与えることができ、用途が限定されてしまう不都合を防ぐことができるようになる。

【図面の簡単な説明】

【図１】本発明の一実施形態である映像入力装置の構成を示すブロック図である。

【図２】本実施形態による映像入力装置の一例であるディジタル・カメラの構成を示すブロック図である。

【図３】本実施形態による映像入力システムの構成例を示すブロック図である。

【図４】出力形式が映像データとディジタル署名との合成である場合のデータの例を示す図である。

【図５】ディジタル署名のみを出力する場合の映像入力システムの構成例を示すブロック図である。

【図６】出力形式がディジタル署名のみの場合のデータの例を示す図である。

【符号の説明】

imaging method　撮像部

memory for control program　制御ソフトウェア記憶用のメモリ部

work memory　ＣＰＵの作業用のメモリ部

operation switch　操作部

motor　機構動作部

memory for recorded data　映像データのメモリ部

external I/F　外部装置とのインターフェイス

C-CODEC　ディジタル署名生成部

ＩＭＧ　撮像部

ＰＲＣ　画像処理部

ＣＰＵ　中央演算装置

ＲＯＭ　読みだし専用のメモリ部

ＤＲＡＭ　読み書き可能なメモリ部

ＳＴＲＧ　映像データや音声データを記録するメモリ部

ＣＯＤＥＣ　ディジタル署名生成部

Ｉ／Ｆ　外部装置とのインターフェイス

ＰＣＭＣＩＡ　外部装置とのＰＣＭＣＩＡ規格に基づくインターフェイス

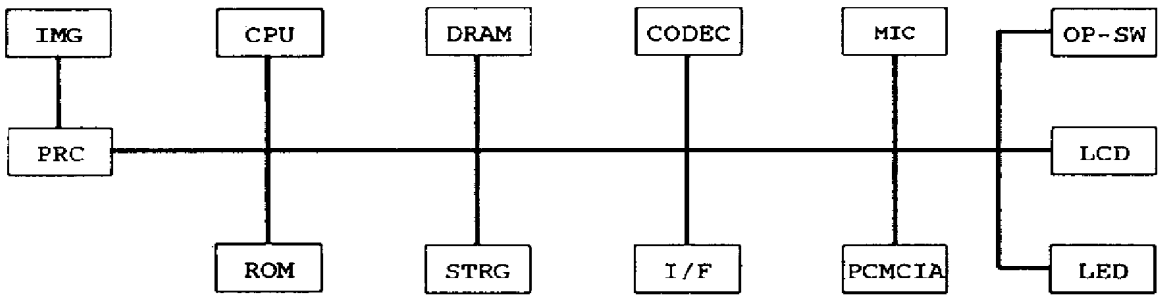
ＭＩＣ　音声入力部

ＯＰ－ＳＷ　操作部

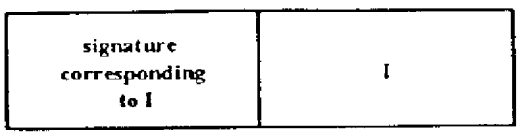
ＬＣＤ　ディスプレイ

ＬＥＤ　ランプ

【図２】

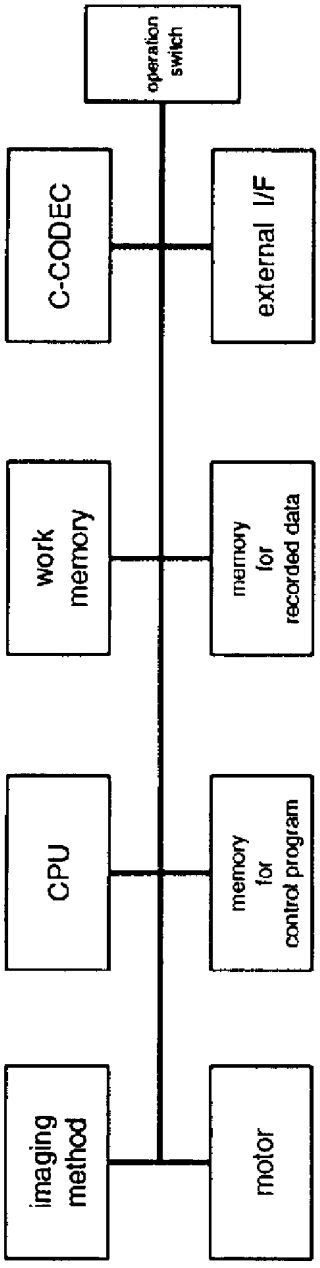


【図４】



【図６】

【図１】


operation switch
C-CODEC
external I/F
work memory
memory for recorded data
CPU
memory for control program
imaging method
motor

【図３】

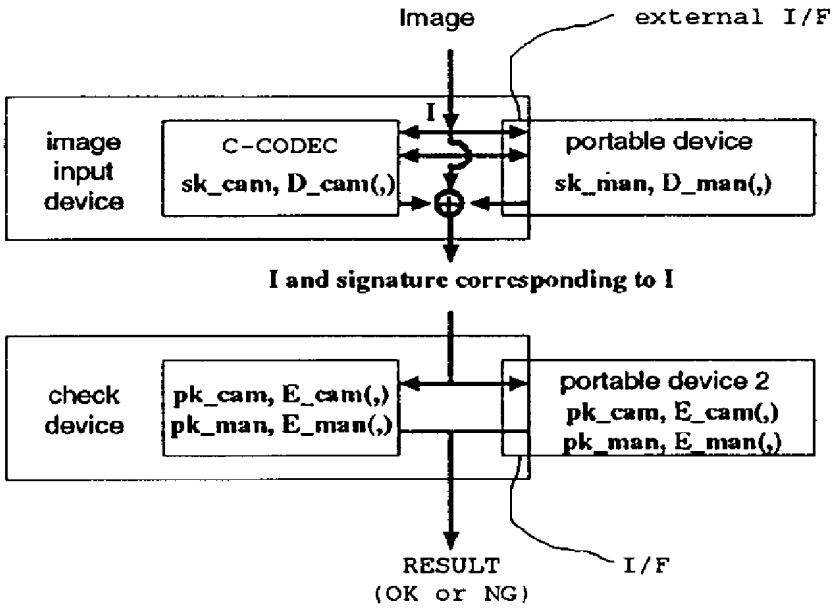


Image
external I/F
I
image input device
C-CODEC
sk_cam, D_cam(,)
portable device
sk_man, D_man(,)
I and signature corresponding to I
check device
pk_cam, E_cam(,)
pk_man, E_man(,)
portable device 2
pk_cam, E_cam(,)
pk_man, E_man(,)
RESULT
(OK or NG)
I/F

【図５】

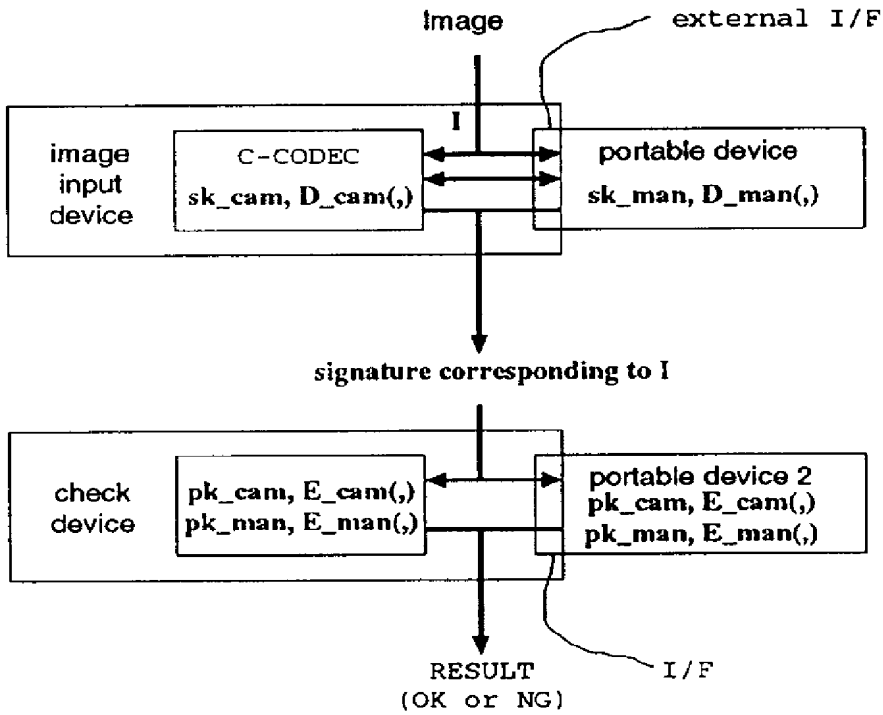


Image
external I/F
I
image input device
C-CODEC
sk_cam, D_cam(,)
portable device
sk_man, D_man(,)
signature corresponding to I
check device
pk_cam, E_cam(,)
pk_man, E_man(,)
portable device 2
pk_cam, E_cam(,)
pk_man, E_man(,)
RESULT
(OK or NG)
I/F

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
// Ｈ０３Ｍ　7/30			Ｈ０４Ｎ　5/91	Ｐ	